REMARKS

The Examiner is thanked for the comments in the Action. They have helped us considerably in understanding the Action and in drafting this Response thereto.

It is our belief that claims 1-27 remain pending in this application.

We note for the record that the present application is part of a series of applications having priority extending as early as Apr. 25, 2000. The present Action cites Andivahis, which was filed Feb. 5, 2002; and Favazza, which claims benefit of a provisional application filed Jul. 26, 2002. Applicant reserves its right to remove these references as prior art in the event the remarks below are deemed unpersuasive.

We proceed now with reference specifically to the numbered items in the Action.

Items 1, 3, 6, and 10: These are informational in nature and are understood to require no reply.

Item 2 (IDS):

The Action correctly notes that a Written Opinion (dated 22 DEC 2005) was listed in but omitted from our last IDS. A first new IDS is provided herewith that includes this reference.

The same foreign examining authority has recently issued a second Written Opinion (dated 17 JAN 2007). This cites a patent reference (U.S. Pat. No. 6,009,173 by Summner) that may not be of record in this case (although it has been cited and is of record in parent case 10/305,726). A second new IDS is provided herewith that lists both of these references, and that includes a copy of the second Written Opinion as well as an appropriate certification.

Items 4-5 (§ 112, ¶1 rejections):

Claims 1, 5, 14, 19, 23, and 26 are rejected as failing to comply with the written description requirement. Respectfully this is error.

The Action here states "*The claim(s) contains subject matter which was not described in the specification .... The Applicant ... has not explicitly disclose what exactly an "*authentication assertion*" is and what is included in the authentication assertion in the application as filed.*" This is incorrect. For example, paragraph [0255] states:

> *... the authentication authority **418** issues ... an authentication assertion **422**.* [It] *signs this assertion **422** (typically, using a PKI private key). The*

> *assertion **422** includes the identity of the transacting party **412**; the identity of the authentication authority **418**; the validity period of the authentication assertion **422**; and optional confirmation data, used by the key server **420** to prove that the transacting party **412** is the rightful owner of the assertion **422**. One example of such confirmation data may be ....*

As for the physical nature of the authentication assertion, the context of the invention is digital communications via networks such as the Internet. Accordingly, one of ordinary skill in the art would readily appreciate that an authentication assertion is digital data.

Continuing, the Action states that claims 2-4, 6-13, 15-18, 20-22, 24-25 and 27 inherit the deficiencies of claims 1, 5, 14, 19, 23 and 26. For the reasons just stated, however, we also urge that none of these claims are deficient.

Item 7 (§ 103(a) rejections):

Claims 1-27 are rejected as being unpatentable (obvious) over Andivahis in view of Favazza. Respectfully this is error.

As a preliminary item, in Item 7 the Action rejects claim 8 under § 103(a) yet fails to state any supportive argument.

As another preliminary item, the Action states one set of arguments on page 6 (top) and a conflicting second set of arguments on page 7 (bottom) for rejecting claims 15, 22, and 27.

And as another preliminary item, the Action states one set of arguments on page 6 (bottom) and a conflicting second set of arguments on page 7 (bottom) for rejecting claim 17.

Turning now to claims 1, 5, 14, 19, 23, and 26, with respect to these the Action states that "*Andivahis teaches a method ... comprising: (a) receiving a request for a transaction identifier ..., wherein said request includes a source authentication assertion; (col. 4, lines 22-37)*" (underline here and hereinafter added for emphasis). What Andivahis' actually teaches here, however, is "*an authentication process ... between a sender **210** and the key server **240**,*" and this does not use a authentication assertion (i.e., an already existing assertion issued by an authority). In the cite here Andivahis teaches that its "*sender sends an authentication request message to the key server and the latter responds with a number of strings of random bits, one such string to be used for each message sent to the key server.*" This is necessary in Andivahis, yet has no equivalent in Applicant's claims because, by virtue of already having an authentication assertion, Applicant's source does not need to send a message to a key server to get a supply of random bit

strings that only that key server can then recognize. Note also, once Andivahis' sender has such a supply of bit strings, these are not authentication assertions because they do not assert anything.

By way of analogy, an authentication assertion can be viewed as similar to a drivers license or a passport, and random bit strings can be viewed as similar to individual tickets from rolls of generic carnival ticket stock. The following discussion uses these analogies sparingly.

Continuing, the Action next states [that Andivahis teaches] "*(b) verifying said source authentication assertion; (col. 4, lines 40-45).*" Here even more clearly, however, it can be seen that Andivahis is not teaching the use of an authentication assertion. The cite states "*the sender is authenticated,*" but the distinction between being authenticated and doing that with an authentication assertion has apparently been missed. For example, much like Andivahis' key server can be expected to recognize one of its random bit strings, if I appear at my mother's door I will be recognized and she will let me in. In contrast, if I appear at a U.S. border crossing without at least a drivers license or a passport I am probably not 'getting in.'

The Andivahis cite here further states that "*Authentication may entail, for example, checking the sender's identifying information, such as the sender's e-mail address and making sure that the sender is registered with the system,*" but this is not authentication based on an authentication assertion. Reduced to the absurd, I can register the domain name QueenOfEngland@SomeISP.com but that does not mean that I am her royal majesty or that SomeISP.com is asserting that I am. Authentication assertions work because they are based on "*the identity of the authentication authority*" (paragraph [0255], quoted above), not because the security they provide is based on a sender's identifying information.

Continuing, the Action next states [that Andivahis teaches] "*(c) storing said transaction identifier and information from said source authentication assertion, thereby establishing information making the transaction source unable to plausibly repudiate once it encrypts and sends the transaction; (col. 4, lines 61-col. 5, line 9).*" First, there is an illogic on the face of this. How can Andivahis' random bit strings include information? Claim 1 recites "*information from said source authentication assertion*" because information in the authentication assertion there can be retrieved from it and stored. In contrast, the only relevant information a random bit string can provide does not come '*from*' it, rather, it has to be based on it being recognized or not. Second, the Andivahis cite here discusses numerous elements and steps as being necessary to work, yet these have no equivalents in claim 1. For example,

> *the key server **240*** [consulting a] *database to retrieve information about* [a] *recipient **220** identified in recipient public key request* [and preparing] *a recipient public key response **252** which preferably includes ... a data field comprising the recipient's **220** preferred public encryption key ....* [and] *Finally, the key server **240** sends the recipient public key response **252** to the sender **210**.*

Continuing, the Action next states [that Andivahis teaches] "*(d) providing said transaction identifier in reply to said request so that the transaction and said transaction identifier can be sent to the transaction target; (col. 4, lines 61-col. 5, line 9).*" However, the cite here does to support the assertion. Andivahis merely says here that "*The key server ... prepares a recipient public key response* [preferably including] *a message identifier to track the message.*"

Continuing, the Action next states [that Andivahis teaches] "*(e) receiving a second request for a decryption key to decrypt the transaction once it has been received by the transaction target, wherein said second request includes said transaction identifier and a target authentication assertion; (col. 6, lines 24-29).*" However, up to the last underlining, the cite here also does not support the assertion. Notably, there is nothing whatsoever in the cite that is equivalent to a second request, or one specifically for a decryption key. And with respect to the target authentication assertion, all that the Andivahis cite here has is discussion of target authentication that (as pointed out above with respect to the source and step (a)) is not based on an authentication assertion.

Continuing, the Action next states [that Andivahis teaches] "*(f) verifying said target authentication assertion; (col. 6, lines 45-49)* [and] *(g) storing information from said target authentication assertion with the transaction identifier; (col. 6, lines 50-67).*" These are error for the same reasons pointed out above with respect to the source and steps (b) and (c).

Continuing, the Action next states [that Andivahis teaches] "*(h) providing said decryption key in reply to said second request so that the transaction can be decrypted, thereby establishing information making the transaction target unable to plausibly repudiate being a recipient of the transaction. (col. 6, lines 50-67).*" However, here as well, Andivahis does not teach many elements/limitations that it is being relied upon for, while it instead teaches many elements/limitations as being necessary which Applicant's claims do not recite and which Applicant's invention does not need to provide its benefits. For example, as emphasized above, claim 1 has a step (h) where a decryption key (not merely one part of multiple key fragments) is provided in response to a request. Yet Andivahis teaches that in its "*step **562** ... the key server **240** retrieves the archived second split-key fragment Kse2 referenced by Kr* [and] *sends a key*

*fragment retrieval response **258** back to the recipient* [that] *preferably includes ... the second split-key fragment.*" Accordingly, if Applicant's claim 1 recites whole keys and Andivahis teaches fragmented keys, it seems clear that Andivahis is teaching away from what Applicant is claiming. Alternately, temporarily ignoring the incorrect statements in the Action about Andivahis' benefits, the apparent fact that Applicant's claims uses fewer and simpler elements/limitations to achieve its benefits shows that these claims are at least directed to a patentable improvement over Andivahis.

Continuing, the Action next states that:

> [1] *Andivahis does not explicitly disclose receiving a first request includes an authentication assertion.* [2] *Favazza* [2a] *in analogous art, however, discloses a first request includes an authentication assertion. (page 1, paragraphs 9 and 10)* [3] *Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Andivahis with Favazza in order to have a system that enables sharing information in a secure environment by utilizing assertions that are embedded in transport and messaging networks.*

With respect to [1], it is factually correct -- Andivahis does not teach a request that includes an authentication assertion. However, as discussed above, the rationale for this rejection has been based on the incorrect conclusion that Andivahis does teach authentication assertions. So is Favazza here being relied upon only for teaching a request?

With respect to [2], it is generally correct factually. But [2a] is a conclusion, and an irrelevant one. That a reference be "*analogous art*" is not the legal standard. Rather, the applicable standard is:

> *To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure.* MPEP §§ 706.02(j), 2143

Up to [3], Item 7 of the Action has argued points only relevant to the '*all limitations*' criteria. We are now at the end of Item 7 and this needs to mean that [3] includes argument that the other two criteria ('*suggestion/motivation*' and '*expectation of success*') are met. Otherwise, the Action has filed to state a *prima facie* case for obvious here and Applicant's claims 1-27 should be allowable.

Does [3] argue that there is a suggestion or motivation to combine Andivahis and Favazza? Although not stated as such in the Action, [3] appears to be an attempt at this by showing advantages shared with the claimed invention and we proceed on that basis. The '*shared advantage approach*' (as this argument structure is sometimes termed in the patent profession) is not a license to merely consider shared general advantages and to ignore specific advantages of a claimed invention that are not shared. Here in [3], this is apparently what is happening. An advantage like "*sharing information in a secure environment*" is shared, yet it has apparently been overlooked that the claimed invention provides nonrepudiation, audit, the other advantages stated in paragraphs [0035]-[0037], and yet others noted throughout the application, and that the Action does not even imply that the Andivahis and Favazza combination provides these. Ignoring all else, this alone is a powerful showing that Applicant's invention is at least a patentable improvement.

Stated alternately, if Applicant's claimed invention successfully provides advantages like nonrepudiation, audit, etc. If the Action fails (as it does fail) to assert that Andivahis and Favazza in combination successfully provide these advantages, then the '*expectation of success*' criteria has also not been met.

In summary, we urge that the Action fails to completely state and adequately support a *prima facie* case for obvious here and Applicant's claims 1-27 should be therefore be allowable.

Regarding claims 2, 6, 20, and 24, we urge that these are allowable for at least the reasons provided above for parent claims 1, 5, 19, and 23.

Regarding claims 3, 7, 9, 12, 21 and 25, we first urge that these are allowable for at least the reasons provided above for parent claims 1, 5, 19, and 23.

Further, the Action here states that "*Andivahis further discloses a method ... comprising: ... (j) retrieving at least some of said information from said source authentication assertion stored in said step (c) ... (col. 6, lines 57-67; col. 18, lines 25-67).*" However, since Andivahis teaches random bit strings rather than source authentication assertions, as discussed above, it cannot further be teaching retrieving information from an authentication assertion. Nothing in the new Andivahis cites provided here contradicts this.

Regarding claims 4, 15, 22 and 27, we first urge that these are allowable for at least the reasons provided above for parent claims 1, 14, 19, and 26.

Further, the Action here states that "*Andivahis further discloses a method ... comprising: ... (j) determining if said information ... matches with any said information from said target authentication assertion stored with ... (col. 18, lines 25-67).*" However, since Andivahis teaches random bit strings rather than target authentication assertions, as discussed above, it cannot further be teaching retrieving information from an authentication assertion. Nothing in the new Andivahis cite provided here contradicts this.

Regarding claims 10 and 16, we first urge that these are allowable for at least the reasons provided above for parent claims 5 and 14.

Further, the Action here states that "*Andivahis further discloses a method* [including] *storing ... and ... providing said decryption key, thereby facilitating decryption of the transaction by a party* [that] *is not the transaction source or a target of the transaction. (col. 4, line 46-col. 6, line 15).*" However, the Andivahis cite here merely teaches providing an encryption key or providing a one of multiple split key fragments of a decryption key, and it does not teach or reasonably suggest how only such can permit non-source and non-target, third-party decryption.

Furthermore, the manner of citation here fails to meet the Office's requirement "*to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to reply*" (MPEP 706.02(j)). The 'blanket' cite used here extends across considerable text and includes multiple entire paragraphs that are irrelevant. For example, most of the cite deals with the handling of message recipients that are unregistered in Andivahis' system.

Yet furthermore, aside from this being irrelevant to furthering the present rejection, it undermines the rejection by showing that Andivahis clearly suffers from many of the prior art disadvantages that Applicant discusses in paragraphs [0016]-[0025] of the application and which the claimed invention does not suffer from.

Regarding claims 11 and 17, we first urge that these are allowable for at least the reasons provided above for parent claims 5 and 14.

Furthermore, the Action here states that "*Andivahis further discloses a method wherein: said information request received in said step (e) also includes the transaction; and said step (g) includes decrypting the transaction before providing said source information in reply to said information request. (col. 4, line 46-col. 6, line 15).*" However, in addition to the problems noted above with respect to claims 10 and 16, we see no support in the cite that Andivahis teaches or reasonably suggests sending its messages to its key server for decryption and information extraction there. If we have overlooked such support, we respectfully call upon the Examiner to cite its location with specificity.

Regarding claims 13 and 18, we first urge that these are allowable for at least the reasons provided above for parent claims 5 and 14.

Furthermore, the Action here states that "*Favazza further discloses ... step (g) includes also providing the transaction in decrypted form in said reply to said information request, thereby facilitating a* [non-source and non-target, third-] *party making said information request being able to confirm the content of the transaction ... (page 3, paragraphs 40-43).*" However, the cite either fails to support the assertion or Favazza's XML document here has been confused with Applicant's transaction that is exchanged between a source and a target. The XML document is used in a process whereby Favazza's client initially requests something equivalent to an authentication assertion for use in its web session context. However, the only plausible relevance this has to Applicant's claim 13 is to something prior to step (a) in parent claim 5 where a source authentication assertion already exists and is being used. Similarly, the only plausible relevance this has to Applicant's claim 18 is to something prior to step (a) in parent claim 14 where a target assertion already exists and is being used.

Regarding claims 15, 17, 22 and 27 being argued again in the Action under Item 7, we first urge that these are allowable for at least the reasons provided above for parent claims 14, 19, and 16; and we second urge that these are additionally allowable for at least the reasons provided above that our first sets of responsive remarks.

Item 9 (§ 102(b) rejections):

Claims 1, 5, 14, 19, 23, and 26 are rejected as being anticipated by Linehan. Respectfully this is error.

The Action here states, "*Linehan teaches a method for a transaction source and ... target to exchange a transaction that cannot be repudiated ... comprising: (a) receiving a first request for a transaction identifier ..., wherein said request includes a source authentication assertion; (col. 7, lines 30-38; col. 9, lines 25-41).*" However, it appears that a transaction identifier (e.g., a message identifier) has been confused here with a user identifier. The Linehan cites teach only the latter, which is simply irrelevant to the present issues.

Reiterating: authentication assertions work because they are based on "*the identity of the authentication authority*" (paragraph [0255], quoted above), not because the security they provide is based on a sender's (or a receiver's) identifying information. In fact, none of claims 1, 5, 14, 19, 23, and 26 recite that the identities of either a source or a target are known. This is intentional, because it is simply not necessary that party's identities be known to each other or even to the authentication authority or authorities used (which incidentally are other major advantage of the claimed invention over the prior art).

Continuing, the Action states [that Linehan teaches] "*(c) storing said transaction identifier and information from said source authentication assertion, thereby establishing information making the transaction source unable to plausibly repudiate once it encrypts and sends the transaction; (col. 7, lines 40-53; col. 9, lines 25-41).*" However, the Linehan cites fail to support the assertion. Linehan here merely teaches database entry of information that identifies data files being stored in encrypted form. If an encrypted data file is somehow felt to be analogous to Application's transactions, and if storing an encrypted data file is somehow felt to be analogous to Application's source and target exchanging a transaction, what then does it mean to be unable to plausibly repudiate? And what role does a source authentication assertion have in this? In the cites Linehan is teaching personal key based encryption on a user's own personal computer.

Continuing, the Action next states [that Linehan teaches] "*(d) providing said transaction identifier in reply to said request so that the transaction and said transaction identifier can be sent to the transaction target; (col. 7, lines 54-67; col. 9, lines 25-41).*" Here Linehan's Kerberos ticket is apparently confused with Applicant's transaction identifier. This is wrong, however, because in Linehan its "*Kerberos or KryptoKnight tickets are used to identify the user to the*

Personal Key Server when the file is created or accessed" (col. 7, ln. 34-36) and Applicant's transaction identifier identifies its transaction, i.e., a message rather than a message source or target.

Further, Applicant's transaction and transaction identifier are ultimately sent together to the transaction target, whereas in Linehan a ticket is needed to access a stored encrypted file. In Linehan it would seriously undermine security for its files (and render its invention pointless) to send a ticket-and-file combination somewhere together.

Continuing, the Action states [that Linehan teaches] "*(h) providing said decryption key in reply to said second request so that the transaction can be decrypted, thereby establishing information making the transaction target unable to plausibly repudiate being a recipient of the transaction. (col. 6, lines 50-67; col. 9, lines 42-58).*" However, the Linehan cites fail to support the assertion. Even in its own context, Linehan teaches nothing here that one of ordinary skill in art would understand as establishing information such that a recipient of one of its decryption keys could not deny having received that key, or as establishing information such that a recipient could not deny having used such a key to access a file.

In summary, we urge that the Action fails to completely state and adequately support a *prima facie* case for anticipation here and Applicant's claims 1, 5, 14, 19, 23, and 26 should be therefore be allowable.

CONCLUSION

Applicant has endeavored to put this case into complete condition for allowance. It is thought that the §112 rejections have been shown to be unfounded, that the §102 rejections are also shown to be unfounded on the prior art reference cited, and that the §103 rejections have been completely rebutted. Applicant therefore asks that all objections and rejections now be withdrawn and that allowance of all claims presently in the case be granted.

Intellectual Property Law Offices
1901 S. Bascom Ave., Suite 660
Campbell, CA 95008

Telephone: 408.558.9950
Facsimile: 408.558.9960

Respectfully Submitted,

Raymond E. Roberts
Reg. No.: 38,597